SCS評価制度対応を経営課題として進めるべき理由

受注維持・営業競争力・取締役の説明責任・企業信用への影響を実務から解説

サプライチェーン強化に向けたセキュリティ対策評価制度（以下「SCS評価制度」）への対応は、情報システム部門だけに任せる認証取得作業ではない。取引先から選ばれ続けるための条件を整え、事故時の事業停止と信用毀損を抑え、経営陣が合理的な監督を行ったことを説明できる状態をつくる経営課題である。

とりわけ従業員100〜1,000名規模の企業は、大企業の重要な委託先である一方、専任人材や予算が限られやすい。制度運用が始まってから一斉に規程、証跡、技術対策を整えるのでは間に合わない可能性がある。現時点で要求事項との差分を把握し、受注上の優先度と実際のリスクに沿って改善計画を組むことが重要だ。

結論

SCS評価制度対応の本質は「星を取ること」ではなく、重要取引を守るために、経営判断・組織運用・技術対策を証拠とともに整えることにある。最初に目標段階と適用範囲を決め、ギャップ評価、改善、技術検証、申請準備を一つのプロジェクトとして管理したい。

この記事で分かること

- SCS評価制度の概要と、★3・★4で想定される評価の違い
- 受注維持、営業競争力、取締役の説明責任、企業信用との関係
- 経営層と情報システム部門が準備すべき事項、資料、進め方
- Webアプリケーション診断、プラットフォーム診断、ペネトレーションテストを使い分ける考え方
- 費用・期間を左右する要因、支援会社を選ぶ際の確認点

SCS評価制度とは何か

SCS評価制度は、サプライチェーンを構成する企業のセキュリティ対策を共通の物差しで可視化する制度である。経済産業省と内閣官房国家サイバー統括室の監督の下、独立行政法人情報処理推進機構（IPA）が運営する。委託元が取引契約などで委託先に必要な段階（★）を示し、その実施状況を確認する利用場面が想定されている。

制度が解こうとしているのは、発注側には『委託先の対策を把握しにくい』、受注側には『顧客ごとに異なる質問票へ回答する負担が大きい』という双方の問題だ。共通基準が定着すれば、発注側は確認を標準化し、受注側は自社の対策を再利用可能な形で説明しやすくなる。

★3と★4の違い

段階	評価の考え方	経営上の位置づけ
★3	セキュリティ専門家の確認を経た自己評価。経営層による自己適合宣誓を含む。	すべてのサプライチェーン企業が最低限備えるべき基礎を整える起点。
★4	登録された評価機関による第三者評価。技術検証も組み込まれる。	重要な機能・情報・接続を担う企業が、組織的かつ継続的な対策を外部に示す手段。
★5	要求事項、評価スキーム、開始時期を検討中。	現時点で取得計画の前提にせず、公式情報の更新を確認する。

IPAの2026年5月29日更新FAQでは、★3・★4は2027年3月頃の運用開始予定とされ、取得には各段階で定められたすべての要求事項・評価基準を満たす必要がある。申請方法や解説書などは順次公開予定であり、公開時期や細部は変更され得るため、最新の公式情報を確認したい。

出典：**IPA**『**SCS**評価制度』：https://www.ipa.go.jp/security/scs/index.html

出典：**IPA**『**SCS**評価制度の詳細情報』：https://www.ipa.go.jp/security/scs/details.html

出典：**IPA**『よくある質問』：https://www.ipa.go.jp/security/scs/faq.html

なぜ**SCS**評価制度対応を経営課題として進めるべきなのか

1. 受注維持に影響し得るから

SCS評価制度は法律によってすべての企業へ一律に取得を義務付ける制度ではない。しかし、取引契約などで委託元が委託先に必要な段階を示す利用が想定されている以上、実務上は調達条件、更新審査、取引先評価の一部になる可能性がある。重要顧客が★3または★4を要請したとき、準備がなければ回答期限に間に合わず、追加説明や是正計画を求められる。場合によっては新規案件への参加や契約更新で不利になり得る。

経営層が把握すべきなのは、どの顧客がいつ要請しそうか、対象売上と粗利はいくらか、代替困難なサービスを提供しているか、顧客システムへの接続や機密情報の取扱いがあるかである。取得費用だけを見るのではなく、『未対応によって影響を受ける売上・取引』と比較して投資判断する必要がある。

2. 営業競争力と信用の共通言語になり得るから

法人営業では、セキュリティ質問票への回答、監査の受入れ、規程や診断報告書の提出が受注前のボトルネックになりやすい。営業担当が『対策しています』と説明しても、適用範囲、実施頻度、責任者、記録が曖昧なら信用にはつながらない。SCS評価制度に沿って対策と証跡を整理すれば、営業、法務、情報システム部門の回答が一致し、顧客説明の速度と再現性を高められる。

もっとも、星の取得だけで個別案件の安全性を保証できるわけではない。顧客のデータ、接続方式、委託範囲に応じて追加説明は必要だ。それでも、共通基準を土台にすれば、独自質問票への回答をゼロから作る負担を減らし、営業活動で『何を、どこまで実施しているか』を具体的に示せる。

3. 取締役が合理的な判断と監督を説明する材料になるから

サイバー事故が起きたという結果だけで、直ちに取締役の法的責任が確定するわけではない。責任は個別事情により判断される。一方、経済産業省のサイバーセキュリティ経営ガイドラインは、経営者が認識すべき原則と、責任者へ指示すべき事項を示しており、サプライチェーン全体の状況把握と対策も重要項目に含めている。

したがって取締役会では、制度対応の担当部署を決めるだけでなく、重要資産・重要取引、許容できる停止時間、投資額、未解消リスク、重大事故時の報告経路を定期的に確認したい。議事録、承認済み方針、リスク評価、改善計画、演習記録を残すことは、平時の実効性を高めるだけでなく、事故後に『どの情報を基に、何を判断し、どのように監督したか』を説明する基盤になる。

出典：経済産業省『サイバーセキュリティ経営ガイドライン **Ver3.0**』：https://www.meti.go.jp/policy/netsecurity/mng_guide.html

参考：**IPA**『指示**9** ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策』：
https://www.ipa.go.jp/security/economics/practices_navi/practice236.html

4. 事故対応と事業継続の準備を同時に進められるから

サプライチェーン攻撃では、自社の端末感染だけで問題が終わらない。盗まれた認証情報が顧客環境への侵入に使われる、受発注システムが停止して供給が滞る、共有ファイルから設計情報が漏れる、改ざんされたソフトウェアや更新ファイルが顧客へ配布される、といった波及が起こり得る。

制度対応を経営課題として扱えば、予防策だけでなく、検知、封じ込め、復旧、顧客通知、証拠保全、代替業務まで含む事業継続の議論ができる。これはITの復旧手順にとどまらず、納期、売上、違約金、広報、個人情報保護、取引先への報告を横断するテーマである。

対応しなかった場合に起こり得る問題

未対応の影響は、制度開始日に突然発生するとは限らない。まず顧客調査への回答が遅れ、次に是正要求や追加監査が増え、最終的に入札・更新条件との不一致が顕在化するという段階的な形が考えられる。特に問題なのは、技術対策を導入していても、対象範囲や運用記録がなく『実施を証明できない』状態だ。

また、脆弱性を放置したインターネット公開機器、共有管理者ID、バックアップの同一ネットワーク保管、退職者アカウントの残存、委託先権限の未棚卸しなどは、ランサムウェアや不正侵入の被害を拡大させる。事故時に契約上の報告期限や連絡先が分からなければ、技術的復旧が進んでも顧客対応が遅れ、信用を損なうおそれがある。

対象となる企業・システム・場面

制度はサプライチェーンを構成する企業全体を対象としている。従業員数だけで対象可否を判断するのではなく、取引上の役割とリスクを見るべきだ。製造業の部品会社、物流会社、BPO、クラウド・SaaS事業者、システム開発・運用会社、保守会社、データ処理会社などは、顧客の事業継続や情報保護に直接影響しやすい。

優先度が高いのは、顧客ネットワークへの接続がある、個人情報・営業秘密・設計情報を預かる、停止すると顧客の生産やサービスが止まる、ソフトウェアや更新物を提供する、再委託先が多い、といった場面である。自社全体を無条件に対象とするのではなく、組織、拠点、業務、システム、クラウド、委託先の境界を明文化し、除外する範囲には合理的な理由を持たせる。

SCS評価制度対応の具体的な進め方

ステップ1：経営目的と目標段階を決める

最初に『顧客から求められたから』だけでなく、守る取引、改善したいリスク、目標時期、目指す★を経営会議で合意する。主要顧客の調達方針が未公表なら、営業部門がヒアリングし、契約更新月や次年度予算の時期を把握する。★3から始めるのか、重要サプライヤーとして★4を見据えるのかで、必要な体制と技術検証の深さが変わる。

ステップ2：適用範囲と責任体制を定める

対象は法人名だけでなく、拠点、部門、業務、情報資産、ネットワーク、クラウドサービス、顧客接続、再委託先まで具体化する。責任者には権限と予算を与え、経営層、情報システム、セキュリティ、法務、総務、人事、営業、事業部門の役割を決める。100〜1,000名規模では専任組織がない場合も多いため、外部専門家を使う範囲も先に線引きしたい。

ステップ3：要求事項とのギャップを評価する

規程の有無だけでなく、実際の運用と証跡を確認する。例えばアカウント管理なら、規程があるかに加え、申請・承認、定期棚卸し、退職者停止、特権ID監視の記録を見る。脆弱性管理なら、資産台帳、情報収集、優先順位、修正期限、例外承認、再確認がつながっているかを確認する。

この段階で準備したい資料は、組織図、情報セキュリティ方針・規程、資産台帳、ネットワーク構成図、クラウド一覧、アカウント・権限一覧、委託先一覧と契約、インシデント対応計画、教育記録、バックアップ・復旧試験記録、脆弱性診断報告書、ログ監視記録、リスク台帳、取締役会・経営会議の承認記録などである。資料が存在しても更新日や対象が一致しなければ、証跡として弱い。

ステップ4：リスクと受注影響で改善順位を付ける

改善項目は件数順ではなく、①顧客・事業への影響、②攻撃される可能性、③外部公開や特権などの露出、④法令・契約・評価基準との不一致、⑤改善に要する期間で優先順位を付ける。重大な脆弱性、インターネット公開機器の多要素認証未導入、復旧不能なバックアップ、事故連絡網の欠落は、文書整備より先に暫定対策が必要な場合がある。

経営報告では、専門用語の一覧ではなく、『止まる業務』『影響する顧客』『想定損失』『暫定措置』『恒久対応の期限』『リスク受容者』へ翻訳する。未解消リスクを黙って残さず、誰がいつまで受容するかを明確にする。

ステップ5：技術的な実効性を検証する

文書と設定表だけでは、実際に攻撃経路を遮断できるか分からない。Webアプリケーション診断は、顧客向けWebシステムや管理画面に対し、認証不備、アクセス制御、SQLインジェクションなどの脆弱性を確認する。プラットフォーム診断は、サーバー、ネットワーク機器、OS、ミドルウェアの設定不備や既知脆弱性を確認する。

ペネトレーションテストは、合意したシナリオの下で複数の弱点を組み合わせ、重要資産へ到達できるかを検証する。単体の脆弱性一覧では見えにくい侵入後の横展開や権限昇格を確認できる一方、対象・時間・停止リスクの調整が必要だ。すべての企業に同じ検証を当てるのではなく、SCS評価の目標段階、顧客接続、重要資産、過去の診断結果に合わせて選ぶ。

ステップ6：証跡を整え、模擬評価を行う

改善後は、要求事項、社内ルール、実施記録、責任者、保存場所を対応付ける。規程だけを新設して運用開始前の状態で申請準備を終えないことが重要だ。サンプルを抽出し、承認記録、ログ、教育受講、パッチ適用、復旧試験、委託先確認が同じ説明と整合するかを模擬評価する。

ステップ7：申請後も継続運用する

評価はゴールではない。組織変更、新システム、M&A、クラウド移行、主要委託先変更があれば適用範囲とリスクを見直す。定期的な脆弱性診断、重大変更後の再診断、ログ監視、教育、インシデント対応演習、バックアップ復旧試験を年間計画へ組み込み、経営層へ指標と例外を報告する。

実施期間と費用を左右する要因

必要期間は、目標段階、適用範囲、既存のISMS等の運用成熟度、拠点・システム数、文書と証跡の整備状況、改修の難易度、評価機関等の日程によって変わる。初期診断だけなら数週間で整理できる場合があるが、規程改定、認証基盤刷新、ネットワーク分離、ログ基盤整備、復旧試験まで必要なら数か月以上を見込むべきだ。制度運用開始直前は専門家・評価機関への依頼集中も想定されるため、余裕を持って着手したい。

費用は『申請の支援費』だけでは決まらない。現状評価、プロジェクト管理、規程整備、教育、ツール導入、設定変更、診断・ペネトレーションテスト、是正支援、再検証、第三者評価などに分けて見積もる。複数拠点や多数のクラウド、海外子会社、OT環境、顧客ごとに分かれたネットワークがあると工数は増える。逆に、資産台帳と責任者が明確で、既存のISMSや監査証跡を再利用できれば効率化しやすい。

社内稟議で説明すべき内容

稟議では『制度対応が必要』という抽象的な説明では予算化しにくい。対象顧客と売上、要求される可能性のある段階、現在の不足、事故時の事業影響、対応しない場合の選択肢、対応期間、概算費用、社内工数を一枚で示す。費用はセキュリティ部門のコストではなく、受注維持、監査対応効率化、事業継続、顧客信用を支える投資として整理すると、営業・事業部門との合意を得やすい。

同時に、星の取得を売上増加の確約として扱わないことも大切だ。投資効果は、対象売上の防衛、質問票回答時間の短縮、重大脆弱性の解消率、復旧目標の達成、顧客監査の指摘減少など複数の指標で追う。

サービス提供会社の選び方

支援会社は、評価基準の読解だけでなく、組織・技術・経営の間をつなげられるかで選ぶ。RFPまたは見積依頼では、目標段階、適用範囲、成果物、社内外の役割、現地確認の有無、技術検証の方法、是正支援、再確認、制度変更時の追随、機密情報の管理、再委託、担当者の資格・経験を確認したい。

成果物には、適用範囲、要求事項別の判定と根拠、証跡一覧、リスク評価、改善優先順位、担当・期限を含むロードマップ、未解消事項、経営層向け要約を含める。『チェックリストを埋めて終わり』ではなく、発見事項を実装・運用へ落とし、再検証まで伴走できる会社が望ましい。★3の確認者や★4の評価機関には制度上の登録要件があるため、正式な評価を依頼する段階ではIPAの公表情報で登録状況を確認する。

よくある失敗と注意点

規程だけを短期間で増やす

ひな形を自社名に置き換えても、実際の承認経路、ツール、担当者、記録と一致しなければ運用できない。現場へのヒアリングとサンプル確認を行い、守れる規程にする必要がある。

適用範囲を広げすぎる、または狭めすぎる

全社一括で始めて停滞する例もあれば、評価を通しやすくするために重要システムを不合理に除外する例もある。顧客へのサービス提供と情報の流れを起点に、境界と依存関係を説明できる範囲を設定する。

診断結果を件数だけで管理する

脆弱性の深刻度だけでなく、悪用可能性、外部公開、保有データ、業務影響、代替策を組み合わせて判断する。改修できない場合は、アクセス制限や監視強化などの代替策と受容期限を決める。

情報システム部門だけで進める

委託先契約は法務、顧客要求は営業、教育は人事、事業継続は各事業部門が関与する。部門横断の責任体制がなければ、文書と実態がずれ、顧客説明も統一されない。

評価対応と機密情報管理を切り離す

支援会社や評価者へ、構成図、脆弱性、ログ、顧客情報など高機密の資料を渡す場合がある。秘密保持、アクセス制御、保管場所、暗号化、再委託、保存期間、返却・削除、事故時報告を契約と運用の両面で確認する。

Librus株式会社が提供できる支援

Librus株式会社は、SCS評価制度への対応方針の整理から、現状評価、適用範囲の設計、規程・証跡の整備、改善計画、技術検証、運用定着まで一気通貫で支援する。制度の要求事項を満たすためだけでなく、企業ごとの事業、顧客、システム、予算、組織体制に合わせて実行可能な形へ落とし込む。

技術面では、Webアプリケーション診断、プラットフォーム診断、ペネトレーションテスト、レッドチーム演習、SOC／CSIRT構築、インシデントレスポンス、デジタルフォレンジックなどを組み合わせられる。経営面では、リスクアセスメント、取引先監査、M&A・IPOなどの重要局面を踏まえ、経営層、情報システム部門、現場部門の間で判断基準をそろえる。

既にISMSや社内規程がある企業には既存資産を生かした差分対応を、体制が未整備の企業には優先順位を絞った段階的な導入を提案する。診断結果を提出して終わるのではなく、改善の実装、再診断、継続監視、教育・演習まで支援できる点が特徴である。

よくある質問

Q1. SCS評価制度への対応は法律上の義務ですか？

すべての企業に一律の取得義務を課す制度ではありません。ただし、委託元が取引契約や調達条件で必要な★を示す利用が想定されているため、自社の主要顧客や業界の方針を確認する必要があります。

Q2. ★3と★4のどちらを目指すべきですか？

顧客から求められる段階、自社が扱う情報、顧客環境への接続、供給停止時の影響で判断します。まず★3の基礎を整え、重要サプライヤーとして★4を見据える段階計画も考えられます。

Q3. ISMSを取得済みなら追加対応は不要ですか？

不要とは限りません。既存の規程や証跡を再利用できる可能性はありますが、SCS評価制度の要求事項、適用範囲、評価方法との対応関係を確認し、不足を補う必要があります。

Q4. SCS評価制度の運用開始はいつですか？

IPAの2026年5月29日更新FAQでは、★3・★4は2027年3月頃の運用開始予定です。申請方法などは順次公開予定のため、最新の公式情報を確認してください。

Q5. 準備にはどのくらいの期間がかかりますか？

初期のギャップ評価は数週間で整理できる場合があります。ただし、規程整備、システム改修、運用記録の蓄積、技術検証を含めると数か月以上かかることがあります。

Q6. 脆弱性診断だけで対応できますか？

脆弱性診断は重要ですが、それだけでは十分ではありません。ガバナンス、資産・権限管理、委託先管理、教育、ログ監視、インシデント対応、復旧など組織と運用の対策も必要です。

Q7. どのシステムを診断対象にすべきですか？

顧客データを扱うシステム、インターネット公開システム、顧客ネットワークへ接続する端末・機器、認証基盤、事業停止の影響が大きい基盤を優先します。適用範囲とリスク評価から決めるのが基本です。

Q8. まだ対象範囲や予算が決まっていなくても相談できますか？

可能です。主要顧客、提供サービス、情報・システムの流れを確認し、目標段階、優先範囲、概算スケジュールを整理するところから始められます。

まとめ：SCS評価制度対応は取引と事業を守る経営基盤

サプライチェーン強化に向けたセキュリティ対策評価制度、SCS評価制度への対応は、単なるチェックリスト対応ではない。受注維持と営業競争力を支え、事故による停止と信用毀損を抑え、取締役が合理的な判断と監督を説明できる状態をつくる取り組みである。

経営層は目標段階、対象取引、適用範囲、許容リスク、予算を判断し、情報システム部門は資産、設定、運用記録、診断結果を整える。営業、法務、人事、事業部門を巻き込み、要求事項との差分をリスクと受注影響で優先順位付けすることが、無理のない対応につながる。制度の細部は今後も更新されるため、公式情報を確認しながら早期に現状把握を始めたい。

SCS評価制度対応の進め方を整理したい企業へ

Librus株式会社では、要求事項とのギャップ評価、目標段階と適用範囲の設計、経営層向け説明、規程・証跡整備、脆弱性診断やペネトレーションテスト、改善ロードマップの策定まで相談できる。対象システムや実施方法が決まっていない段階でも、主要取引と事業リスクから優先順位を整理することで、過不足のない計画を立てやすくなる。

CTA案1｜まずは現状と要求事項の差を可視化する

制度対応の全体像が見えない場合は、既存の規程、運用、システム対策を確認し、要求事項との差分を整理するところから相談できる。対応が必要な項目と既存資産を切り分けることで、予算と社内工数の見通しを持ちやすくなる。

CTA案2｜重要取引から対応範囲を絞り込む

すべてを一度に進める必要があるか判断できない場合は、主要顧客、契約更新時期、取扱情報、顧客環境への接続状況を基に優先範囲を設計できる。受注維持とリスク低減の両面から、経営会議や稟議で説明しやすい計画へまとめる。

CTA案3｜技術対策から改善・運用定着まで相談する

診断の要否や対象が未確定でも相談可能である。Webアプリケーション診断、プラットフォーム診断、ペネトレーションテストなどをリスクに応じて選び、発見事項の優先順位付け、改善、再検証、継続運用まで一貫して進めることで、評価対応を実効性のあるセキュリティ強化につなげられる。

監修者

鎌田光一郎：青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先

Librus株式会社（代表取締役 鎌田光一郎）

〒105-0004 東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F

電話：03-6772-8015

お問い合わせフォーム：https://librus.co.jp/contact

主な公的情報・一次情報

IPA『**SCS**評価制度』：https://www.ipa.go.jp/security/scs/index.html

IPA『**SCS**評価制度の詳細情報』：https://www.ipa.go.jp/security/scs/details.html

IPA『要求事項・評価基準』：https://www.ipa.go.jp/security/scs/requirements-criteria.html

IPA『よくある質問』：https://www.ipa.go.jp/security/scs/faq.html

経済産業省『サイバーセキュリティ経営ガイドライン』：https://www.meti.go.jp/policy/netsecurity/mng_guide.html

IPA『サイバーセキュリティ経営ガイドライン **Ver3.0**実践のためのプラクティス集』：https://www.ipa.go.jp/security/economics/csm-practice.html